Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. - 2.   (canceled)

3. (previously presented) A client platform as claimed in claim 25, wherein the client trusted component contains an integrity monitor adapted to provide a measure of the integrity of code operating on the client platform, and the integrity monitor is adapted to monitor the integrity of the image receiving code.

4. - 5.   (canceled)

6. (previously presented) A client platform as claimed in claim 25, wherein the client platform further comprises a secure user interface for providing user input directly to the client trusted component, and wherein the image receiving code is adapted to provide user input received from the secure user interface to a server.

7. (previously presented) A client platform as claimed in claim 25, wherein the client trusted component is adapted to authenticate other trusted components or secure tokens.

8. (previously presented) A client platform as claimed in claim 25, wherein the client trusted component is adapted to determine a trusted status of other platforms.

9. (previously presented) A client platform as claimed in claim 25, also comprising a smart card reader for receiving a Smart card comprising a user's secure token.

10. (previously presented) A client platform as claimed in claim 25, wherein a part of the display is reserved for display of data determined by the server independent of any request by the client platform.

11. – 14. (canceled)

15. (previously presented) A system as claimed in claim 28, adapted for a user to request execution of code on the client platform to provide image data to be viewed at the client platform.

16. (previously presented) A system as claimed in claim 25, adapted for a user to request execution of code, and for code then to be executed partly on the client platform and partly on the server to provide image data to be viewed at the client platform, wherein the image data is viewed at the client platform in association with the results of code executed on the client platform.

17. (previously presented) A system as claimed in claim 28, wherein the client platform comprises a smart card reader for receiving a smart card comprising a user's secure token, further comprising a user smart card wherein the server is adapted to determine that the user smart card is such as to allow the image data to be sent to the client platform.

18.   (canceled)

19. (previously presented) A method as claimed in claim 29, further comprising provision of request data from the client platform to the server, and provision of modified image data based on the request data.

20. (original) A method as claimed in claim 19, wherein the provision of request data and the provision of modified image data are repeated as often as required.

21. (previously presented) A method as claimed in claim 29, further comprising updating of a usage log after image data or modified image data is provided to the client platform.

22. (previously presented) A method as claimed in claim 29, wherein the step of determining permission comprises determining whether a smart card containing a user permission is in session with the client platform.

23. (previously presented) A method as claimed in claim 29, wherein a part of the image data is determined by the server independent of any request from the client platform.

24. (original) A method as claimed in claim 23, wherein said part of the imaging data comprises advertising content.

25.   (currently amended) A client platform adapted to provide restricted use of data provided by a server, the client platform comprising:

a display;

a secure communication means;

a client trusted component physically and logically protected from unauthorised modification to provide verification of the integrity of the platform to a user upon user request, the client trusted component having an associated memory containing image receiving code for receiving data from a server by the secure communications means and for display of such data, and further having a display controller such that the display is controlled from within the client trusted component;

wherein the client platform is adapted such that the data received from the server is used for display of the data and not for an unauthorised purpose.

26. (previously presented) A server adapted to provide data to a client platform for restricted use by the client platform, comprising:

a memory containing image sending code for providing an image of data executed on the server;

secure communications means for secure communication of images to a client platform; and

means to authenticate a trusted component of a client platform, the trusted component having a display controller such that display of the data from the server is controlled from within the client trusted component;

whereby the server is adapted to authenticate the trusted component of a client platform to determine that said client platform is adapted to ensure restricted use of the data before it is sent by the image sending code.

27. (previously presented) A server as claimed in claim 26,

containing a server trusted component physically and logically protected from modification, wherein said server trusted component contains the means to authenticate a trusted component.

28. (previously presented) A system for providing image data securely to a user for restricted use, comprising:

a client platform comprising a display, a processor adapted to allow secure communication with remote parties, a client trusted component physically and logically protected from unauthorised modification to provide verification of the integrity of the platform to a user upon user request, the client trusted component having an associated memory containing image receiving code for receiving data securely from a server and for display of such data and further having a display controller such that the display is controlled from within the client trusted component; and

a server comprising a memory containing image sending code for providing an image of data executed on the server, a processor adapted to allow secure communication of images to the client platform and to authenticate a trusted component of the client platform;

wherein the server is adapted to authenticate the trusted component of a client platform to determine that said client platform is adapted to ensure restricted use of the data before it is sent by the image sending code, the client platform is adapted such that the data received from the server is used for display of the data and not for an unauthorised purpose, and the system is adapted for a user on the client platform to request image data from the server to view at the client platform.

29. (previously presented) A method of providing image data to a
client platform for restricted use, comprising:

    a client platform requesting image data from a server;

    the server determining that the client platform both has
permission to receive image data, and has a client trusted
component physically and logically protected from unauthorised
modification adapted to use the image data only for the
restricted use and to control display of the image data from
within the client trusted component; and

    provision of the image data over a secure communication
channel.

30. (canceled)